



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Welcome to the CCoE Webinar Series. Our speaker today is Dr. George Strawn. Our host is Jeannette Dopheide.

The meeting will begin shortly. Participants are muted. You may type questions into the chat box during the presentation.

This meeting is being recorded.

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.

Science or Security

George O. Strawn

ISU(retired)

NSF (retired)

NITRD (retired)

NAS

Outline

- Anecdotes about IT security
- Observations about IT security
- Research for next generation IT security

In the beginning...

- When I broke in to this business, IT security meant keeping the machine door locked and putting the backup tapes in another building
- Timesharing on big machines and floppy disks on small ones complicated IT security, but we didn't foresee the future
- The security-free Internet and the Morris worm might have warned us

Post-1995

- At a pitac meeting in the late 1990s, a captain of industry said, "Our customers want simpler and faster networks. Security makes them more complicated and slower. The government will have to take the lead."
- In 2005, the nitrd program stood up the interagency working group, Computer Security and Information Assurance (CSIA)
- The USG as lead customer?

In CIO-land (2003-9)

- I receive assurances that NSF is prepared for a virus...
- I am required to name a senior security official, I make my best decision and we spend our best money
- Privacy joins the party and I become the senior privacy official. PII becomes the acronym of the day and CIA becomes **C**ia

Security and red faces

- Incident one: NSF-funded computers implicated in a major ddos attack. NSF grant to Educause to assist universities with security
- Incident two: Hack attack on a major NSF-supported facility. NSF grant to initiate the series of Security Summits
- Incident three: Hack attack at South Pole Station steals scientific data. NSF invests more in Polar security

Random thoughts

- Cybersecurity is a little like airport security: the first requirements are the appearance of and concern about security
- Cybersecurity is a little like the VA: just because it's underfunded is no excuse for not doing a perfect job
- The people in charge of cybersecurity should keep their necks clean

Observations about security

- Security is a *system property*, where a *system* is an interacting set of components, most of which will be subsystems
- It is easy to create insecure systems from secure components; it is hard to create secure systems from insecure components (but that's the goal)
- IT security (eg, CIA--confidentiality, integrity, availability) relates to a system that includes hardware, software, *human* and other components

Perfection?

- Perfect cybersecurity is as likely as zero-fatality automobile traffic
- Plan for mitigating failures as well as preventing them
- Classify failures: embarrassment, cia, financial loss, loss of life (a cps danger)

Risk Management

Likelihood * Damage

Likelihood. Low. Medium. High.

Damage

Low.	1.	2.	3.
------	----	----	----

Medium.	2.	4.	6.
---------	----	----	----

High.	3.	6.	9.
-------	----	----	----

IT insecurity sources

- Software/hardware/human error (eg, buffer overflow)
- Insider crime
- Social engineering (eg, phishing)
- Third, third, third or quarter, quarter, half?

Crooks and Espionage

- Botnets (spam, ddos and key-stroke capture)
- State versus commercial data theft
- Cyberwar
- Ransomware
- Where are scientific facilities in all this?

Doing the Right Things vs doing Things Right

- A dollar spent on security is a dollar less for science?
- Is economizing on cybersecurity false economy?
- Maximal bang for the cybersecurity buck is an obvious goal
- Remember the crime novel maxim: "If you can't do the time (suffer the consequences of a particular hack), then don't do the crime (of under-investing)"

More random thoughts

- Keep the whole system in focus, not just the IT
- Increase time and attention paid to risk analysis and mitigation
- Cultivate a bad cop from afar (like OMB for the agencies)

NITRD

- An interagency program under OSTP that coordinates the IT R&D programs of 20 U.S. Federal agencies (check out www.nitrd.gov)
- Over \$4 billion annually in agency IT R&D investments, including more than \$700 million in *computer security and information assurance (CSIA)*



Federal Cybersecurity R&D Strategic Plan



TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

Executive Office of the President
National Science and Technology Council

DECEMBER 2011



- Research Themes
 - Tailored Trustworthy Spaces
 - Moving Target
 - Cyber Economic Incentives
 - Designed-In Security
- Science of Cyber Security
- Support for National Priorities
- Transition to Practice



Tailored Trustworthy Spaces

- Paradigm
 - Supporting context-specific trust decisions
 - Basing trust decisions on verifiable assertions
- R&D Program Examples
 - Trusted foundation for cyberspace operations [OSD and Service Labs]
 - High assurance security architectures [NSA, ONR, AFRL, NIST]
 - Content and Context Aware Trusted Router (C2TR) [AFRL]
 - Information Security Automation Program [NIST, NSA, DHS]
 - Security Content Automation Protocol (SCAP) and Access Control Policy Machine [NIST]
 - Military Networking Protocol (MNP) program [DARPA]
 - High-Level Language Support for Trustworthy Networks [NSF]

Moving Target

- Paradigm
 - Providing resilience through agility
 - Continue safe operation in a compromised environment
- R&D Program Examples
 - Polymorphic Enclaves and Polymorphic Machines [AFRL]
 - Self Regenerative, Incorruptible Enterprise that Dynamically Recovers with Immunity [AFRL]
 - Clean-slate design of Resilient, Adaptive, Secure Hosts (CRASH) [DARPA]
 - Mission-Oriented Resilient Clouds [DARPA]
 - Cyber Camouflage, Concealment, and Deception [DARPA]
 - Morphing Network Assets to Restrict Adversarial Reconnaissance (Morphinator) [Army]
 - Defensive Enhancements for Information Assurance Technologies (DEFIANT) [Army]
 - Robust Autonomic Computing Systems [ONR]



Cyber Economic Incentives

- Paradigm
 - Developing understanding of what impacts cyber economics
 - Providing incentives to good security
- R&D Program Example
 - NSF Secure and Trustworthy Cyberspace (SaTC) Program
 - NSF Computer & Information Science & Engineering Directorate + NSF Social, Behavioral & Economic Sciences Directorate

Designed-In Security

- **Paradigm**
 - Developing SW systems that are resistant to attacks
 - Generating assurance artifacts to attest to the system's capabilities to withstand attacks
- **R&D Program Examples**
 - Survivable Systems Engineering [OSD/SEI CERT]
 - Trusted Computing [DARPA, NSA, OSD, NIST]
 - Software Development Environment for Secure System Software & Applications [ONR]
 - META (flows, tools, and processes for correct-by-construction system design) [DARPA]
 - Software Assurance Metrics And Tool Evaluation (SAMATE) [DHS, NIST]

Supporting National Initiatives

- Health IT
- Smart Grid
- Transportation
- Trusted identities
- Cybersecurity education



Science of Security

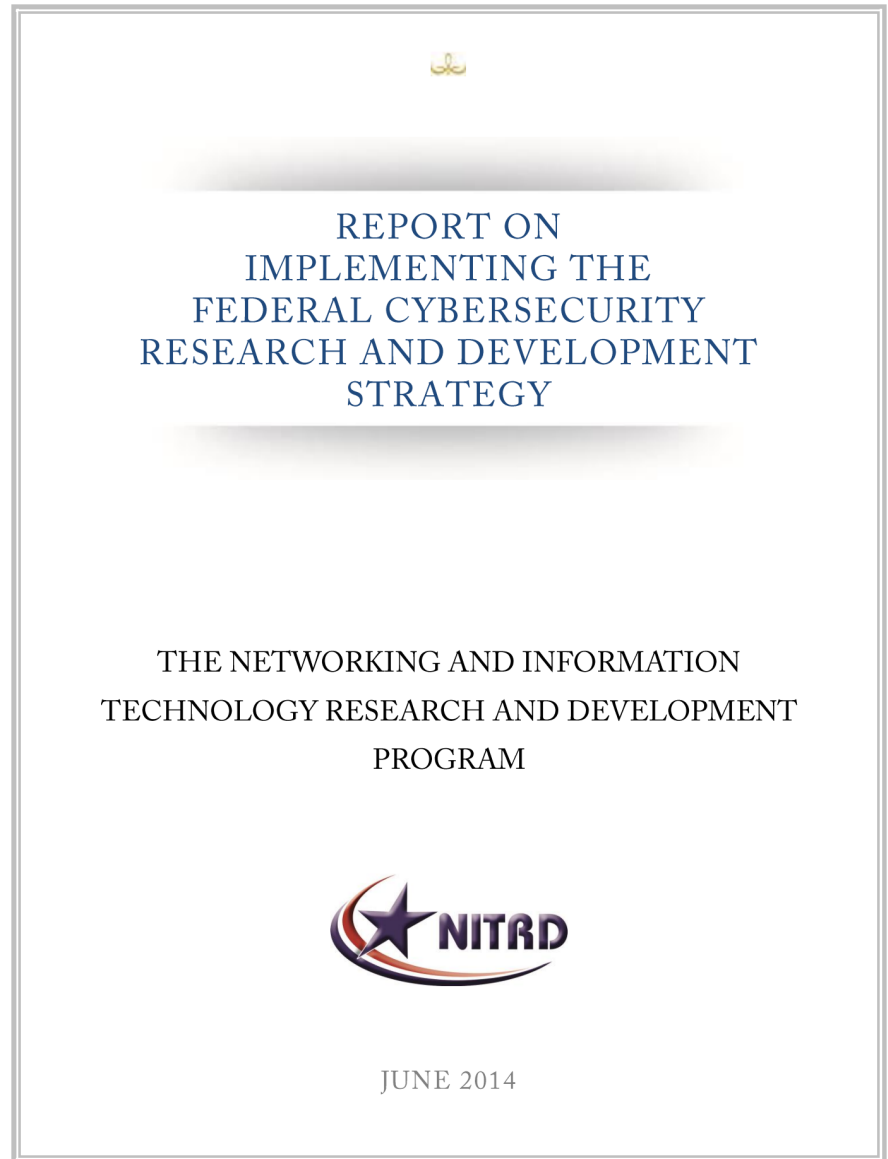
- Paradigm
 - Developing scientific foundations to inform the field of cybersecurity
- R&D Program Examples
 - AFOSR 2011 Science of Security MURI
 - Stanford, Berkeley, Cornell, CMU, U of Penn
 - NSA Science of Security Lablets
 - UIUC, NC State, CMU
 - NSF TRUST Program components
 - Berkeley, CMU, Cornell, San Jose SU, Stanford, Vanderbilt

Accelerating Transition to Practice

- Currently, a chasm exists between the research community and the operations community
- Bridging that chasm, commonly referred to as the "valley of death," requires cooperative efforts and investments by both the R&D and operations communities
- CSRI: Computer Security Research Institute

Next steps

- Assess strategic plan
- Additions and/or deletions



Additions

- Cyberphysical systems
- (IoT)
- Privacy

6.3 Additional Prospective Research Areas

The framework for Federal cybersecurity R&D articulated in the 2011 Strategic Plan is not static; the framework and priorities are expected to evolve as our understanding of challenges and solutions improves. In looking forward, several broad areas of research have emerged as candidates for coordinated, multiagency efforts. While discussion of prospective research areas continues and a decision on priorities remains, examples of additional research that may strengthen the goals of the Strategic Plan are provided below.

6.3.1 Security of Cyber-Physical Systems

Our increasing reliance on cyber-physical systems, in which computing, cyberspace, and control of physical processes are interconnected, requires commensurate advances to secure them and to improve their trustworthiness. Such systems are part of the fabric of modern economies and provide critical functions in areas such as the generation and delivery of electricity, management of transportation systems, and the delivery of medical and emergency care.

Cyber-physical systems operate under constraints arising from the requirements of the physical processes being controlled. Cyber-physical systems are a significant challenge because the traditional ordering of cybersecurity priorities does not hold. Historically, computer systems are designed to meet confidentiality and integrity requirements, with availability as the distant third. For cyber-physical systems, which may be controlling the shut-off valve in a power plant or a water system, availability is often the most important requirement. There are also real-time requirements and other subtleties that differentiate these systems from the cyber world. In the energy sector, for example, stringent, millisecond operational requirements of energy delivery systems cannot be affected adversely by security technologies. Cybersecurity solutions that are developed to protect business systems and networks may not be appropriate for cyber-physical systems; additional research is needed to address requirements specific to these systems.

6.3.2 Privacy and Protected Disclosure

The January 2013 President's Council of Advisors on Science and Technology (PCAST) report on the NITRD Program¹⁶ cited privacy and protected disclosure as a cross-cutting theme, "one that is important for every agency and mission, as huge amounts of diverse information about individuals become available in online electronic form." Multiple public comments emphasized the need for privacy research to address both how the public perceives privacy in the context of cybersecurity and how new cybersecurity technologies and practices can integrate privacy.

As highlighted in the PCAST report, a major challenge is that "no agency has primary responsibility for privacy R&D, although many agencies need a better understanding of the science of privacy and protected disclosure in an online digital world." Development of the scientific and engineering foundations of privacy R&D will require multiagency collaboration.

While some aspects of privacy are included in the scope of the Tailored Trustworthy Spaces theme, there are additional challenges that can be addressed through targeted R&D investment. The challenges, as outlined in the PCAST report, include realizing the benefits of collective personal information without compromising the privacy of individuals, achieving cybersecurity and security more broadly without unnecessary disclosure of individual information, designing systems to avoid unintended personal disclosure, empowering individuals to assert their identity and also to make

¹⁶ <http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd2013.pdf>

More random thoughts

- The "science" of cybersecurity is harder than previous successes like compilers, operating systems, database systems, networking, etc
- The escalating war between the good guys and the bad guys will continue. Cyber science should help the good guys
- Bad publicity helps, but God forbid a cyber disaster

Finally

- Because cybersecurity is still an immature (and ever-changing) discipline, we see through the glass darkly
- Cloud computing has been called the industrialization of IT. To what extent might it be the industrialization of cybersecurity, too?

Thank You!

Questions?

Please take our survey.

About the CTSC Webinar Series

To *view* presentations, *join* the discuss mailing list, or *submit* requests to present, visit:

<http://trustedci.org/webinars>

The next webinar is December 12th at 11am EDT
Topic: CICI Regional Cybersecurity Collaboration projects

The CTSC Webinar Series is supported by National Science Foundation grant #1547272.

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.



CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE
The NSF Cybersecurity Center of Excellence

Thank You

trustedci.org

 [@TrustedCI](https://twitter.com/TrustedCI)

We thank the National Science Foundation (grant 1547272) for supporting our work.

The views and conclusions contained herein are those of the author and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF.